Security Aspects of a Clean Slate Information Oriented Internet Architecture

Nikos Fotiou, Giannis F. Marias and George C. Polyzos

Abstract Publish/Subscribe is a paradigm that continuously receives increasing attention by the research community, mainly due to its information oriented nature. The PSIRP (Publish-Subscribe Internet Routing Paradigm) project aims at developing and evaluating a clean slate architecture for the future Internet, based on this paradigm. Availability, security, and mobility, are considered as core elements in this new form of internetworking and they are not provided as add-ons. This paper highlights the security aspects of PSIRP presenting the security advantages inherited by the pub/sub paradigm as well as the innovating security mechanisms that have been introduced during this project.

1 Introduction

Publish/Subscribe paradigm has been in the spotlight of various research efforts. Its information oriented nature, the decoupling it offers between information providers and information receivers as well as its location-identity split capabilities, have inspired a variety of–mainly overlay–architectures that focus on multicast [5], mobility [14], indirection [25] as well as on caching [15]. PSIRP project[1] is an FP7 EU funded research effort that envisions a clean slate internetworking architecture based on this paradigm. Moreover by abiding to Trust-to-Trust (T2T) principle [3], i.e., all functions take place in trustworthy places, the PSIRP project considers security as a building block of its architecture rather than as an 'add-on'. PISRP is a publish/subscribe architecture enhanced to support the requirements for a scalable, secure and mobility-friendly future Internet architecture.

Publish/Subscribe architectures are mainly composed by three basic components; publishers, subscribers and a network of brokers [7]. Publishers are information

Athens University of Economics and Business, Mobile Multimedia Laboratory, Patision 76, Athens 104 34, Greece, e-mail: {fotiou,marias,polyzos}@aueb.gr

[1] http://www.psirp.org

providers that ‘publish’ information advertisements. Subscribers on the other hand are information consumers that express their interest on specific pieces of information by issuing subscriptions. Brokers are responsible for matching publications with subscriptions and initiate the information forwarding process from information publishers towards information consumers. The broker in which publication-subscription matching takes place is known as the rendezvous point, and therefore the network of brokers is usually referred as the rendezvous network. Publication and subscription operations are decoupled in time and space allowing for the development mobility as well as anonymization mechanisms. Moreover a publication can be provided by multiple publishers and similar subscriptions can be aggregated, creating this way opportunities for multihoming as well as for multicasting.

Inherently publish/subscribe paradigm has many security advantages, compared to the commonly used end-host oriented paradigm. PSIRP harvests the security advantages the publish/subscribe paradigm offers, whilst PSIRP-specific security mechanisms are being developed. The purpose of this paper is to introduce PSIRP as well as to give an overview of its security features. The paper is organized as follows. Section 2 introduces PSIRP's architecture and its core components. Section 3 highlights the security advantages of publish/subscribe paradigm while Section 4 presents the PSIRP-specific security solutions that have been developed. Section 5 outlines related architectures and our conclusions as well as future work are included in Section 6.

2 The PSIRP architecture

The core element of the PSIRP architecture is information; information is everything and everything is information [26]. In PSIRP every piece of information is identified by a unique, flat, self-certified identifier, known as the *rendezvous identifier* (RId). Information is organized in *scopes*. Scopes are physical or logical structures that facilitate the finding as well as access control a over a piece or collection of information. A physical scope can be for example a corporate network, whereas a logical scope can be a group of friends in a social network. Scopes can be included within each other, creating a flexible structure. Scopes are identified by a flat identifier known as the *scope identifier* (SId). Each SId is managed by a rendezvous point (RP) which can be a single *rendezvous node* or a complete *rendezvous network*.

The publication operation in PSIRP involves 3 steps [10]; initially the RId of the publication is created, then the SId of the publication scope is identified. and finally the publication is published in the RP that is responsible for handling this SId. The publication message may also contain *metadata*–such as general information about this publication. Figure 1 shows publication operation, in a PSIRP network, with three scopes; the scope MyUniversity and its sub-scope MyLab and the scope MyFamily. As it can been seen in this figure a publisher issues a publication to the

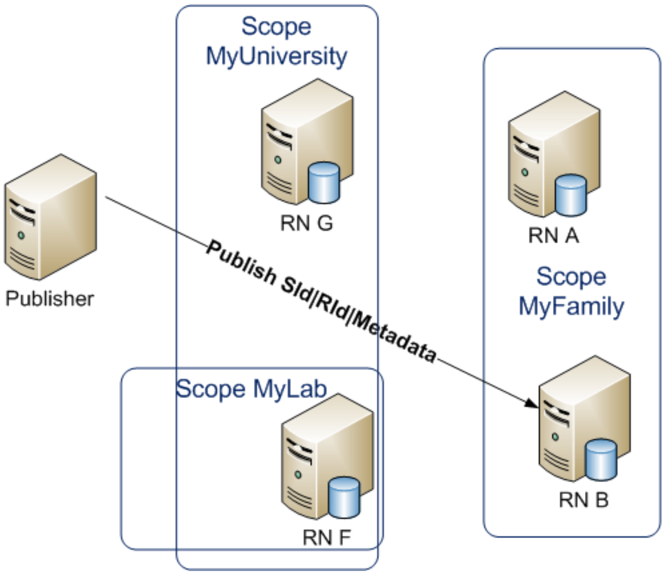

Fig. 1 Publication in a PSIRP network

scope MyFamily. The publication message should contain a scope-unique publication identifier (RId), the MyFamily scope identifier (SId) as well as metadata that describes this publication. The publication message reaches rendezvous node RN B which is part of the MyFamily rendezvous network. The subscription operation involves the identification of the SId and RId of a publication–which can be done for instance, with the help of a search engine–and the sending of a subscription message. Initially the subscription message will be forwarded to the appropriate scope as all the other scopes are not aware of the publication in request. When the subscription reaches the appropriate scope it will be forwarded to the publications RP. The network is responsible for routing publication and subscription messages towards the RP as well as for forwarding publications from publishers towards subscribers. Figure 2 shows subscription operation. A subscriber subscribes to an already published publication. When the subscription message reaches the appropriate RP, and as long as there is a publication that matches this subscription message, the RP creates a forwarding path, from the publisher towards the subscriber, and instructs the publisher to send the publication using the identifier (FId) of this path. PSIRP uses a slow path for signaling, i.e., publication and subscription messages, and a fast path for data forwarding. Moreover multicast is the preferred delivery method in PSIRP.

PSIRP's operation is organized around three basic functions which are recursively executed in all layers of the architecture. These functions are the *Rendezvous*, the *Topology* and the *Forwarding* function [23]. The rendezvous function is responsible for managing an index of publications as well as for providing mechanisms

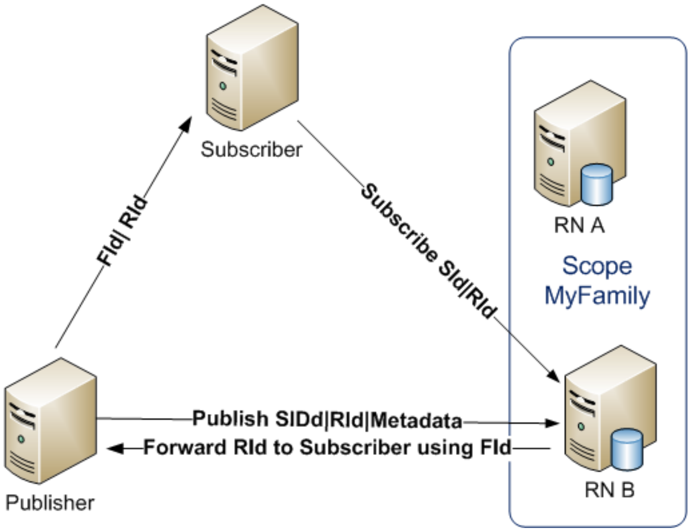

Fig. 2 Subscription in a PSIRP network. Initially the publisher issues a publication, then a subscriber, subscribes to this publication and the rendezvous point instructs the publisher to forward this publication to the subscriber

that enable publication location. In the higher layers of the PSIRP architecture the rendezvous function is distributed and mechanisms such as DHTs and Hierarchical DHTs are used in order to implement it. The topology function is responsible for monitoring the network graph and for creating paths from a publishers towards one– or many (e.g., with the use of multicast)–subscribers. Depending on the layer of the architecture the Topology function can be implemented in a variety of ways ranging from static configuration and simple routing protocols to complex interdomain routing protocols. The forwarding function utilizes the delivery path created by the topology function and forwards data packets. Currently the forwarding function in the higher layers of the PSIRP architecture is implemented using the zFilters [12]; a bloom filter based structure that contains the link identifiers that a data packet must traverse in order to reach its destination(s).

3 Pub/sub security features

The publish/subscribe paradigm can be seen as a remedy to the imbalance of power between senders and receivers, that currently exists. In the current Internet the network will make a best effort to deliver what sender sends, no matter the cost it has for the receiver. This imbalance is often accused for the increasingly number of DDoS attacks as well as for the emerge of spamming. In publish/subscribe systems there is no information flow as long as the receiver has not expressed his interest on a particular piece of information, i.e, the receiver in a publish/subscribe architecture is able to instruct the network which pieces of information shall be delivered to him. Moreover no information is requested from a publisher, unless the publisher has explicitly denote its availability, i.e, unless the publisher has advertise a publication for this particular piece of information.

Publication and subscription operations are decoupled in time and space, i.e., they do not have to be synchronized neither do they block each other. Moreover publishers and subscribers do not communicate directly and they can hide their identity as–in general–subscribers are only interested for the information itself rather than on who provides it, and publishers–usually–disseminate publications using multicast so they cannot be fully aware of the publication's recipients. Therefore anonymity can be easily achieved in publish/subscribe architectures. Moreover by having a point in the network in which subscription and publications are matched, allows for the deployment of access control mechanisms.

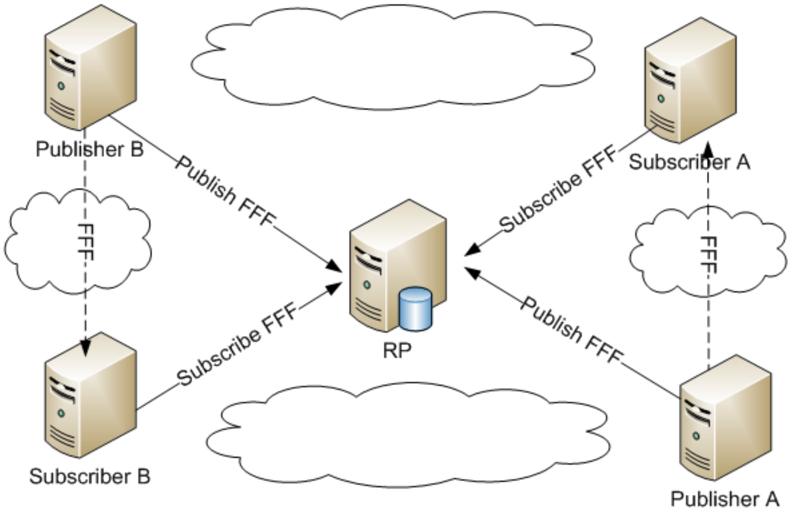

Fig. 3 Example of multihoming in a publish/subscriber architecture

Publish/Subscribe architectures offer great availability. The rendezvous network of a publish/subscribe architecture is usually implemented using a DHT. DHTs provide significant load balancing–usually with the cost of some communication stretch. Moreover in a publish/subscribe architecture multihoming can be easily achieved, as multiple publishers may advertise the same publication to a RP, therefore a RP has a number of options with which it can satisfy a subscription. Figure 3 shows an example of multihoming in a publish/subscribe architecture. Publishers A and B, both publish publication FFF. Subscribers A and B subscribe to this publication. For each subscription message the RP knows two publishers that can provide the publication that matches it, therefore for each subscription message it chooses the publisher that is closer to the respective subscriber, i.e., it chooses publisher A to serve subscriber A and publisher B to serve subscriber B.

Publish/subscribe architectures allow for subscription aggregation and they create chances for multicast, therefore in these architectures resources sharing can be achieved, leading to greater availability. In Figure 4 both subscribers A and B subscribe to the publication FFF. The subscription messages are aggregated inside the networks, as long as they follow the same path towards the RP. Moreover publisher A sends a single data flow, which is copied in a appropriate place in the network in order to serve both subscribers.

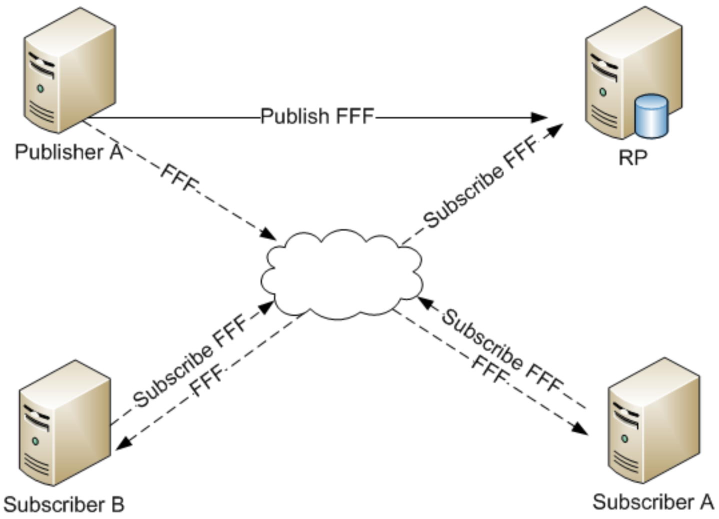

Fig. 4 Resources sharing in a publish/subscribe architecture, using subscriptions aggregation and multicast

4 PSIRP-specific security mechanisms

Security in PSIRP plays an important role and trust is a PSIRP's declared principle. Security mechanisms are considered in all levels of the architecture. Information in PSIRP will by transmitted in encrypted packets usint the Packet Level Authentication (PLA) [19] technique. PLA is a novel mechanism, applied in PSIRP, for protecting the networking architecture based on the assumption that per packet public key cryptographic operations are possible at wire speed in high speed networks due to new cryptographic algorithms and advances in semiconductor technology.

Moreover when applied in wireless environments PLA has been proved to offer significant energy efficiency [20].

As already described PSIRP's forwarding mechanism is based on the formation of a bloom filter–called zFilter–that describes the path that a data packet should follow [12]. The computation of the zFilter is based on the identifiers of the links that compose the data path. These identifiers are dynamically generated every time a zFilter is created, making this way almost impossible for an attacker to create crafted zFilters or link identifiers that will lead DoS attacks or to information leakage. Forwarding using zFilters is achieved in line speed leading to better resources utilization. Network attachment in PSIRP [17] assures proper user authentication protecting both users from improper configuration as well as network from DDoS attacks, that can be caused by malicious users who repeatedly try to attach themselves in a PSIRP network.

In the higher levels of the architecture, existing security mechanisms can be used. Nikkander et al. [22] studied the application of present work on cryptographic protocol analysis in a pure publish/subscribe architecture, i.e., an architecture where all message passing is based on publish/subscribe rather than send/receive, and found out that, even networking protocols are majorly revised, current cryptographic protocol analysis can be applied to a certain extent, with only minor modifications mostly on the notation side. In addition to existing security mechanisms new PSIRP-specific mechanisms are being developed. Multicast and caching are expected to assure PSIRP's architecture availability. Towards this direction a router assisted overlay multicast solution [13] as well as an information oriented caching scheme [16] have been developed, and tested using large scale simulations. Moreover novel trust mechanisms are considered based on information ranking [9] rather than end-users ranking. Information ranking has been proved to be very effective when it comes to malicious information isolation [8].

PSIRP security is going to be greatly enhanced with the notion of scopes. Although not yet implemented, scopes are expected to control information dissemination as well as to play a significant role in applying access control policies as well as accounting mechanisms. Scopes are expected to be PSIRP's information firewalls.

5 Related work

CCNx [6] and 4WARD [1] are two ongoing research projects that investigate the potentials of an information-oriented Internet architecture. In contrast to PSIRP, CCNx proposes an architecture organized using hierarchical naming [11]. Moreover CCNx uses a broadcast-based mechanism for information location, rather than a rendezvous driven one. 4WARD, on the other hand, focuses on network diversity as well as on network self-manageability without diving into core architectural issues.

Data-Oriented Network Architecture (DONA) [18] and Routing on Flat Labels (ROFL) [4] are two pioneering architectures that introduced flat identifiers. DONA aims at replacing DNS with flat self-identifying labels that will enable data location and retrieval, while ROFL creates an internetworking architecture in which routing takes place solely based on the data–flat–identifiers. While PSIRP borrows the information naming concept of DONA, it uses two different paths, a slow and a fast one, for information location and forwarding, respectively. Moreover PSIRP extends ROLF by hierarchically organizing information using scopes.

Internet Indirection Infrastructure (i3) [25] and Host Identity Protocol (HIP) [2] are two rendezvous-based overlay solutions that aim at providing mobility, multicast and multihoming. i3 implements an IP overlay network that replaces the point-to-point communication model with a rendezvous-based paradigm while HIP introduces a new layer, that decouples host identity from location identity, in the internetwork stack between the IP layer and the transport layer . PSIRP's rendezvous and topology processes use similar concepts.

Security in publish/subscribe architectures has received significant attention from the research community. Wang et al. [27] as well as Lagutin et al. [21] have specify security requirements for a publish/subscribe architecture, whereas Wun et al. [28] have identified and classified possible DoS attacks in content-based publish/subscribe systems. Various mechanisms have been developed in order to secure publish/subscribe systems–such as Eventguard [24]–and most of them are based their operation on traditional security mechanisms, that are adapted to the concept of the publish/subscribe paradigm.

6 Conclusion and Future work

In PSIRP project security is not left solely to the significant advantages that the publish/subscribe paradigm offers. In contrast, PSIRP architecture is secured in all layers either by adapting current security mechanisms to a pure publish/subscribe environment or by creating new innovating mechanisms, demonstrating a secure future Internet architecture with high availability.

PSIRP is an ongoing research effort and as it progress and its core components are fain grained, new security mechanisms will be developed. Future work is focused on the creation of a robust, scalable and effective topology manager, that will allow for policies enforcement, on the implementation of a scoping mechanism as well as on the development of an interdomain rendezvous system. Moreover large scale overlay simulations as well as the recently created PSIRP testbed are expected to reveal even more security weaknesses, security requirements as well as new tussles that will guide PSIRP's security research.

Acknowledgements The work reported in this paper was supported by the ICT PSIRP project under contract ICT-2007-216173.

References

1. 4WARD: Web site (2010). `http://www.4ward-project.eu`
2. Al-Shraideh, F.: Host identity protocol. In: Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on, pp. 203 – 203 (2006)
3. Blumenthal, M.S., Clark, D.D.: Rethinking the design of the internet: the end-to-end arguments vs. the brave new world. ACM Trans. Internet Technol. **1**(1), 70–109 (2001)
4. Caesar, M., Condie, T., Kannan, J., Lakshminarayanan, K., Stoica, I.: Rofl: routing on flat labels. In: SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 363–374. ACM, New York, NY, USA (2006)
5. Castro, M., Druschel, P., Kermarrec, A.M., Rowstron, A.: Scribe: a large-scale and decentralized application-level multicast infrastructure. Selected Areas in Communications, IEEE Journal on **20**(8), 1489 – 1499 (2002)
6. CCNx: Web site (2010). `http://www.ccnx.org`
7. Eugster, P.T., Felber, P.A., Guerraoui, R., Kermarrec, A.M.: The many faces of publish/subscribe. ACM Comput. Surv. **35**(2), 114–131 (2003)
8. Fotiou, N., Marias, G., Polyzos, G.: Fighting Spam in Publish/Subscribe Networks Using Information Ranking. In: Proceedings of the 6th Euro-NF Conference on Next Generation Internet Networks (NGI). Paris, France (2010)
9. Fotiou, N., Marias, G., Polyzos, G.: Information Ranking in Content-Centric Networks. In: Proceedings of the Future Network and MobileSummit 2010. Florence, Italy (2010)
10. Fotiou, N., Polyzos, G., Trossen, D.: Illustrating a Publish-Subscribe Internet Architecture. In: In Proceedings of the 2nd Euro-NF Workshop on Future Internet Architectures. Santander, Spain (2009)
11. Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H., Braynard, R.L.: Networking named content. In: CoNEXT '09: Proceedings of the 5th international conference on Emerging networking experiments and technologies, pp. 1–12. ACM, New York, NY, USA (2009)
12. Jokela, P., Zahemszky, A., Esteve Rothenberg, C., Arianfar, S., Nikander, P.: Lipsin: line speed publish/subscribe inter-networking. In: SIGCOMM '09: Proceedings of the ACM SIGCOMM 2009 conference on Data communication, pp. 195–206. ACM, New York, NY, USA (2009)
13. Katsaros, K., Bartsotas, N., Xylomenos, G.: Router assisted overlay multicast. In: Proceedings of the 5th Euro-NF Conference on Next Generation Internet Networks (NGI). Santander, Spain (2009)
14. Katsaros, K., Fotiou, N., Polyzos, G., Xylomenos, G.: Overlay Multicast Assisted Mobility for Future Publish/Subscribe Networks. In: Proceedings of the ICT Mobile Summit. Santander, Spain (2009)
15. Katsaros, K., Xylomenos, G., Polyzos, G.C.: A hybrid overlay multicast and caching scheme for information-centric networking. In: Proceedings of the 13th IEEE Global Internet Symposium. San Diego, CA, USA (2010)
16. Katsaros, K., Xylomenos, G., Polyzos, G.C.: A hybrid overlay multicast and caching scheme for information-centric networking. In: Proceedings of the 13th IEEE Global Internet Symposium. San Diego, CA, USA (2010)
17. Kjallman, J.: Attachment to a Native Publish/Subscribe Network. In: ICC Workshop on the Network of the Future. Dresden, Germany (2009)
18. Koponen, T., Chawla, M., Chun, B.G., Ermolinskiy, A., Kim, K.H., Shenker, S., Stoica, I.: A data-oriented (and beyond) network architecture. In: SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 181–192. ACM, New York, NY, USA (2007)
19. Lagutin, D.: Redesigning internet-the packet level authentication architecture. Licentiates Thesis in Computer Science, Helsinki University of Technology, Espoo, Finland (2008)

20. Lagutin, D., Tarkoma, S.: Public Key Signatures and Lightweight Security Solutions in a Wireless Environment. Smart Spaces and Next Generation Wired/Wireless Networking **5764**, 253–265 (2009)
21. Lagutin, D., Visala, K., Zahemszky, A., Burbridge, T., Marias, G.: Roles and Security in a Publish/Subscribe Network Architecture. In: Proceedings of the 2010 IEEE Symposium on Computers and Communications (2010)
22. Nikander, P., Marias, G.: Towards Understanding Pure Publish/Subscribe Cryptographic Protocols. In: Sixteenth International Workshop on Security Protocols. Cambridge, England (2008)
23. Särelä, M., Rinta-aho, T., Tarkoma, S.: RTFM: Publish/subscribe internetworking architecture. In: Proceedings of the ICT Mobile Summit. Stockholm, Sweden (2008)
24. Srivatsa, M., Liu, L.: Securing publish-subscribe overlay services with eventguard. In: CCS '05: Proceedings of the 12th ACM conference on Computer and communications security, pp. 289–298. ACM, New York, NY, USA (2005)
25. Stoica, I., Adkins, D., Zhuang, S., Shenker, S., Surana, S.: Internet indirection infrastructure. IEEE/ACM Trans. Netw. **12**(2), 205–218 (2004)
26. Tarkoma, S., ed.: PSIRP deliverable 2.3, architecture definition, component descriptions, and requirements (d2.3) (2010). `http://www.psirp.org/`
27. Wang, C., Carzaniga, A., Evans, D., Wolf, A.: Security issues and requirements for Internet-scale publish-subscribe systems. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 3940–3947 (2002)
28. Wun, A., Cheung, A., Jacobsen, H.A.: A taxonomy for denial of service attacks in content-based publish/subscribe systems. In: DEBS '07: Proceedings of the 2007 inaugural international conference on Distributed event-based systems, pp. 116–127. ACM, New York, NY, USA (2007)